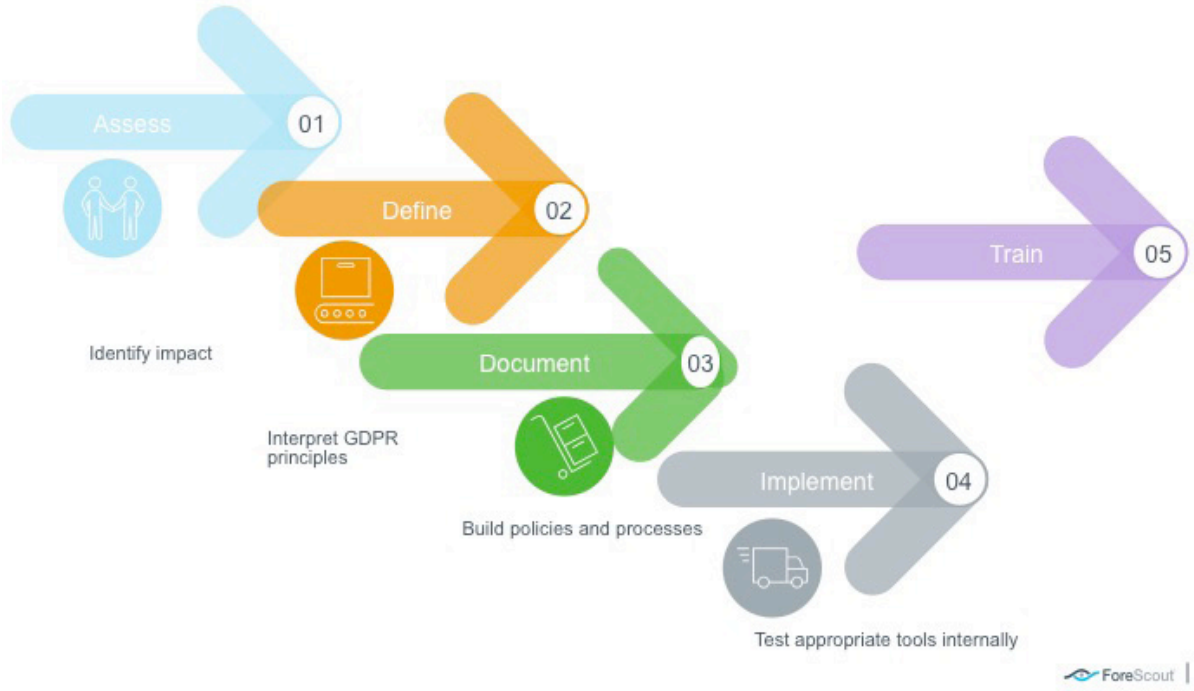
How ForeScout Technologies Is Preparing for GDPR

There is no doubt that the General Data Privacy Regulation (GDPR) will change the way companies worldwide view and handle the personal information of EU citizens and, by extension, individuals in all countries around the globe. GDPR breaches may result in hefty fines, bad publicity and lost revenue. As a multinational corporation with offices in 11 locations globally and more than 2,700 customers worldwide, ForeScout views GDPR as a critical initiative and is taking steps to achieve compliance with the requirements of GDPR.

Early in 2016, the general counsel of ForeScout tasked a cross-functional team to evaluate the GDPR and develop a plan to address its requirements. This document is the culmination of that group's efforts.

We realize that understanding the GDPR text and applying the principles to your own organization can be complicated. To assist our customers, we thought it might be useful to share our experience, thus helping you to simplify your journey into becoming GDPR-compliant. Below is the process we are using and will continue to refine. Our process involved the following five steps:



Step 1. Assess:

As with all regulations, the most important step is identifying the impact of the regulation on the company's existing strategy for managing and mitigating risk. Questions the ForeScout team asked included:

- Do we have the resources internally to efficiently define and implement GDPR requirements? If not, what are the risks involved in outsourcing this work?
- What kinds of personal data, if any, of EU residents does ForeScout collect or use that might apply to the specific guidelines of GDPR?
- What risk to business continuity would a breach of personal data create, and what might be the impact of any resulting fines?
- What benefits might result from achieving compliance under GDPR?
- What processes do we need to change to meet the requirements under GDPR?

ForeScout

- What timelines are realistic within the constraints of the May 2018 deadline?
- What gaps exist and how do we address them?

Step 2: Define:

In this phase, we interpreted and applied the definitions in GDPR Article 4. In this process, the team needed to determine the following:

1) What are the issues and concerns the EU regulators are trying to achieve with GDPR? Do we adequately understand the rights EU residents or data subjects have under GDPR?
2) Do we need a formal Data Privacy Officer?
3) Is ForeScout a Data Controller or Data Processor? Under what circumstances are we using sub-processors?
4) What other laws on privacy have a bearing on what we need to define for GDPR?
5) Based on the types of personal information/data we discovered in step 1, how much effort should we put towards "pseudonymization," or are there equally effective access control methods?
6) Do we have a lawful basis for "cross-border processing"?

Step 3: Document:

The cross-functional team agreed on the construct for a privacy policy for all prospects and customers to assure them of our commitment to GDPR principles. The team also determined the need for better agreements between ForeScout, its data controllers, data processors and applicable sub-processors. The team developed the following:

1) Catalog of personal data we either store or may have access to:
   a. HR – employee data including national IDs and Social Security numbers
   b. Sales – customer contact information
   c. Marketing – leads including name, address and telephone number
   d. Engineering/Product –device IDs, IP addresses
2) External privacy policy – disclosure of information to be collected, how used, how tracked (for example, cookies, mechanism for opt-out)
3) Internal processes for achieving the requirements of GDPR (for example, what technical and organizational measure does ForeScout use to help ensure a level of security appropriate to the risk?) (Article 32)

Step 4: Implement:

Two areas of focus for the team were to internalize and test our interpretation of GDPR both from a human and technical standpoint. Our goal was to build a comfortable environment for our employees who handle personal information while ensuring that our technical controls would support our strategy. Implementation considerations included:

1) The human side of implementation:
   a. ForeScout will leverage a trusted third party to review its processes and procedures in the context of GDPR
   b. As a lawful basis for cross-border transfers, the company will undertake the steps necessary to self-certify under the EU Privacy Shield Framework
2) How ForeScout CounterACT® protects us from privacy breaches today:
   a. Identifying all devices connected to the network that might be storing personal information, including mobile devices
   b. Automating endpoint compliance by identifying and flagging machines without the latest patches and fixes
   c. Monitoring network traffic for clear text user names and passwords
   d. Securing our environment through continuous firewall monitoring

Step 5: Train:

In this phase, we will help our employees understand the context of GDPR, the goal of the Council of the EU in defining the standards for GDPR, and the steps we need to take internally to ensure compliance. Considerations for employee training will include:

1) Marketing – use of leads, posting our privacy policy on our website

2) HR – appropriate access to personal data, implementation of a global privacy policy and notice

3) Engineering – ongoing conversations are planned for continuing to secure machine name, IP address and other data that might be linked back to a person

4) IT and Security – training on continued use of CounterACT to monitor compliance

5) Legal team – continually review the GDPR and related Article 29 Working Papers as well as processes and procedures to maintain awareness and adherence to the goals and objectives of GDPR.

The principles embodied in GDPR represent the ideals that all companies that handle personal data should strive to uphold and enforce. ForeScout plans to engage in continuous knowledge-gathering and successful partnerships, focusing on enabling our customers while protecting valuable information.

Learn more

Addressing the EU General Data Protection Regulation (GDPR) Solution Brief

GDPR: A Europe-Based Regulation with Global Impact white paper

ForeScout Extended Modules for SIEM Solution Brief

EU GDPR home page

ForeScout Technologies offers the unique ability to see devices the instant they connect to the network, control them and orchestrate information sharing and threat response among disparate security tools. Learn how at www.forescout.com.

Learn more at
www.ForeScout.com

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591